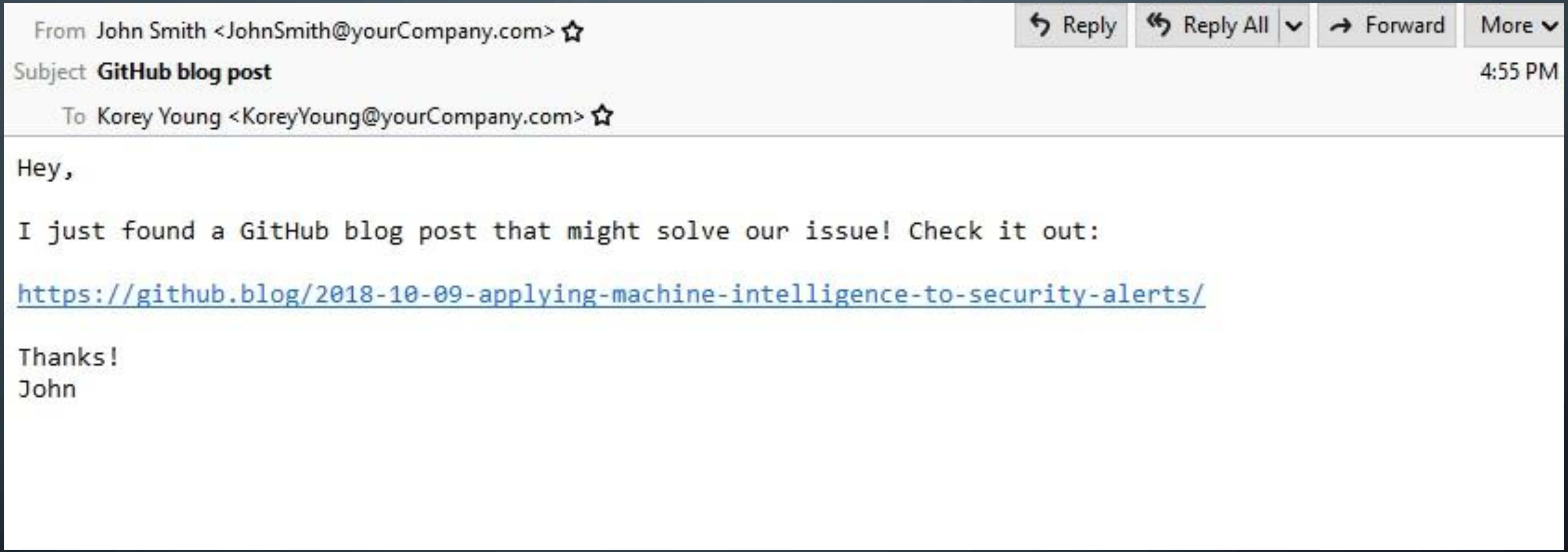
PHISHING GITHUB USERS

WITH OLD BLOG POSTS

ABOUT ME - KOREY YOUNG

- Bloomsburg University – Computer Science.
- But I have always had an interest in cyber security and hacking / red team activities
    - Finding ways to make computers do things that they were not meant to do;
    - So that we can get it fixed before the bad guys discover it and try to use it.
- Dakota State University - Masters in Information Assurance
- SANS GWAPT certification – Web Application Penetration Tester / Ethical Hacker
- My day job is application security engineering for a banking software company, trying to hack into our applications.
- In my free time after work and on weekends, I do cyber security and exploit research.

WOULD YOU CLICK THIS LINK?



From John Smith <JohnSmith@yourCompany.com>

Subject **GitHub blog post**

4:55 PM

To Korey Young <KoreyYoung@yourCompany.com>

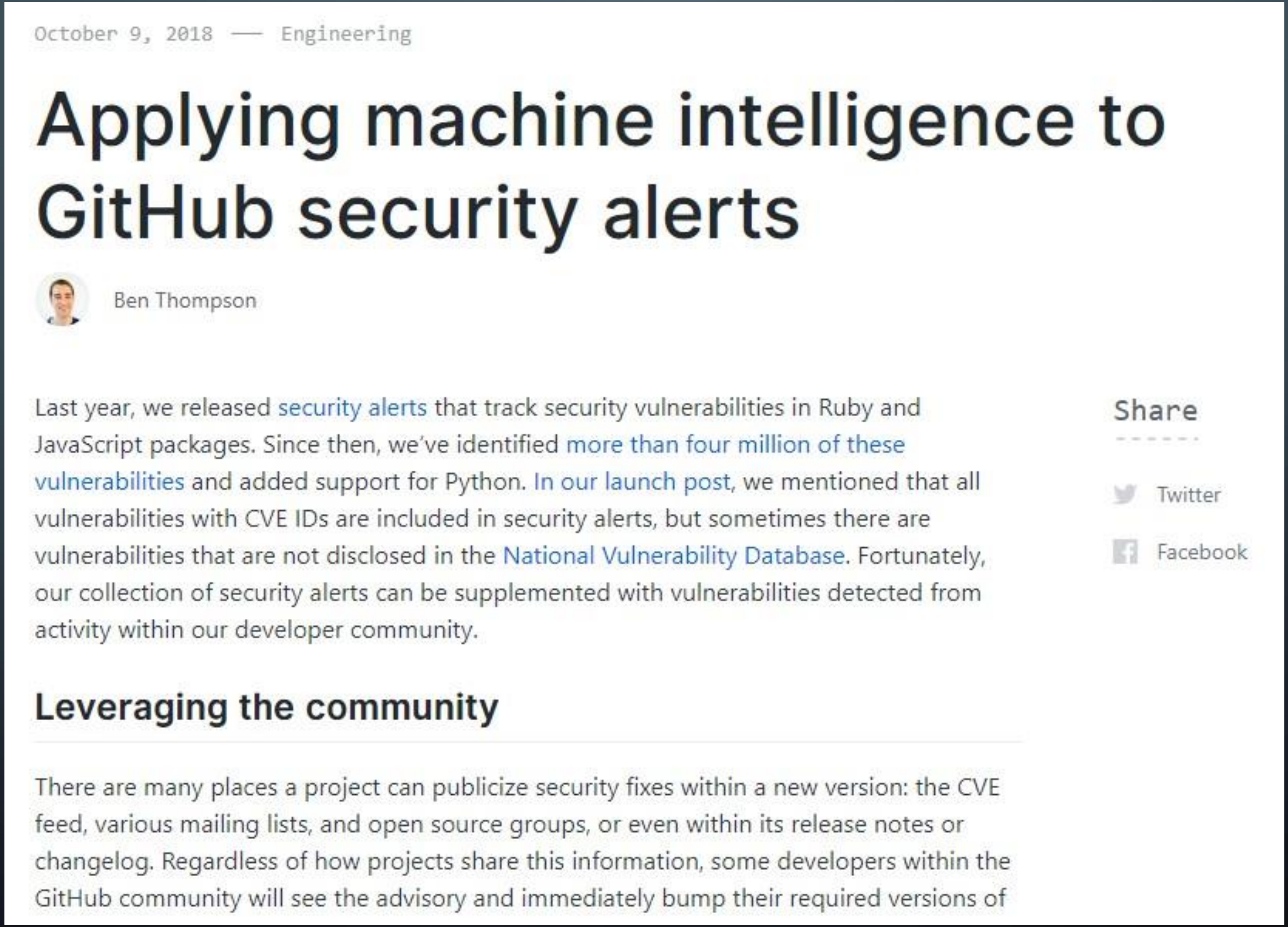
Hey,

I just found a GitHub blog post that might solve our issue! Check it out:

https://github.blog/2018-10-09-applying-machine-intelligence-to-security-alerts/

Thanks!
John

WOULD YOU CLICK THIS LINK?



October 9, 2018 —— Engineering

Applying machine intelligence to GitHub security alerts

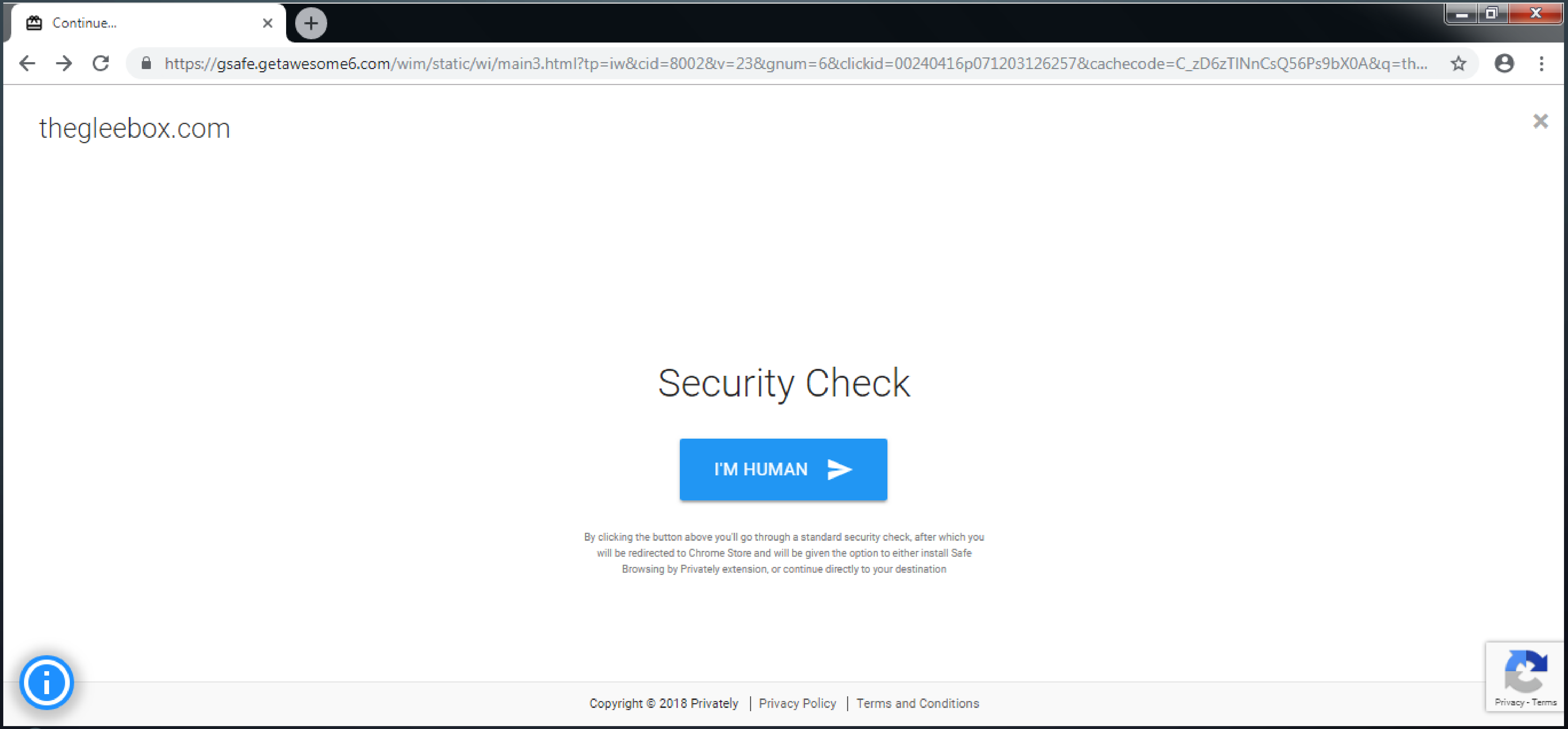
Ben Thompson

Last year, we released security alerts that track security vulnerabilities in Ruby and JavaScript packages. Since then, we've identified more than four million of these vulnerabilities and added support for Python. In our launch post, we mentioned that all vulnerabilities with CVE IDs are included in security alerts, but sometimes there are vulnerabilities that are not disclosed in the National Vulnerability Database. Fortunately, our collection of security alerts can be supplemented with vulnerabilities detected from activity within our developer community.

Leveraging the community

There are many places a project can publicize security fixes within a new version: the CVE feed, various mailing lists, and open source groups, or even within its release notes or changelog. Regardless of how projects share this information, some developers within the GitHub community will see the advisory and immediately bump their required versions of

YOU COULD END UP HERE



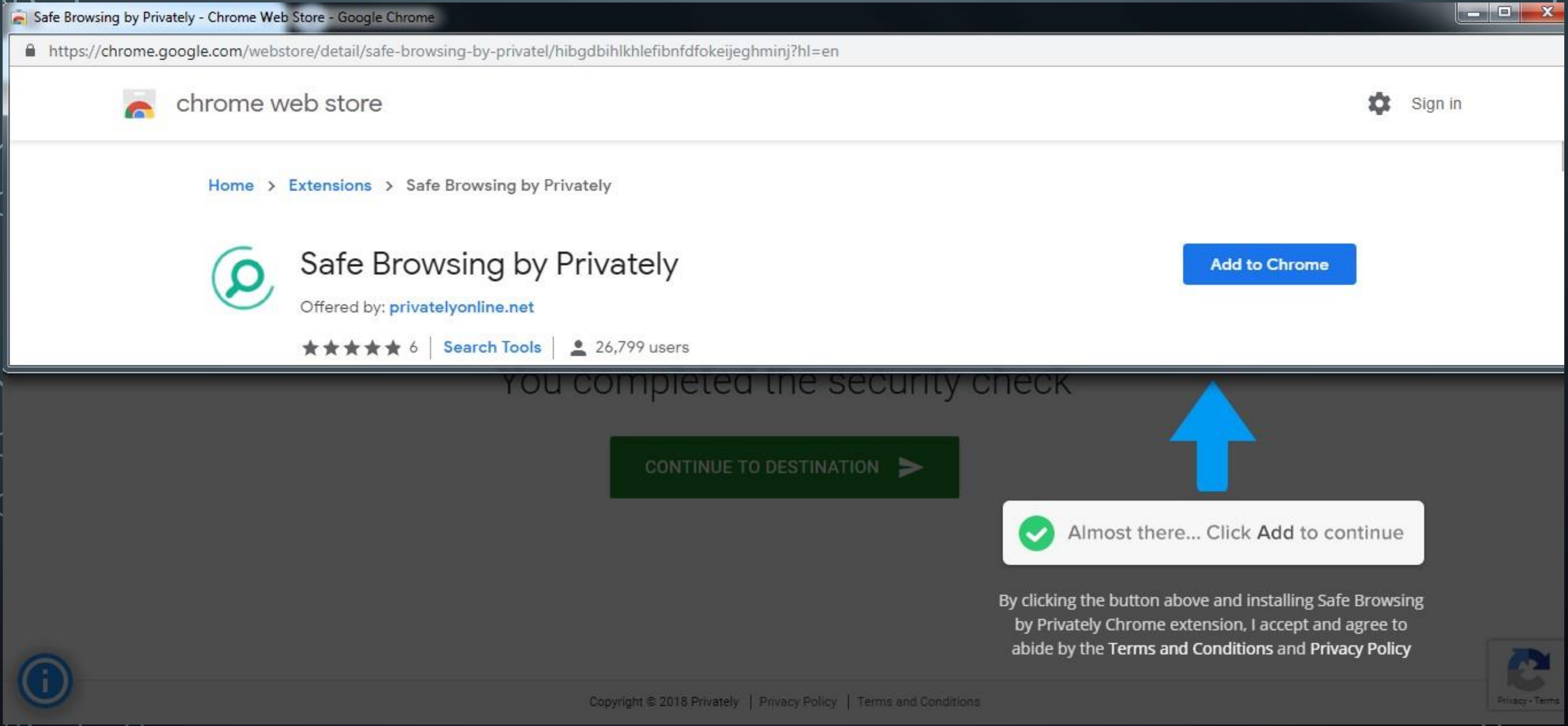
https://gsafe.getawesome6.com/wim/static/wi/main3.html?tp=iw&cid=8002&v=23&gnum=6&clickid=00240416p071203126257&cachecode=C_zD6zTlNnCsQ56Ps9bX0A&q=th...

thegleebox.com

Security Check

By clicking the button above you'll go through a standard security check, after which you will be redirected to Chrome Store and will be given the option to either install Safe Browsing by Privately extension, or continue directly to your destination

Copyright © 2018 Privately | Privacy Policy | Terms and Conditions



Safe Browsing by Privately - Chrome Web Store - Google Chrome
chrome web store
Sign in
Home > Extensions > Safe Browsing by Privately
Add to Chrome
Search Tools
CONTINUE TO DESTINATION

https://chrome.google.com/webstore/detail/safe-browsing-by-privatel/hibgdbihlkhlefibnfdfokeijeghminj?hl=en

Safe Browsing by Privately

Offered by: privatelyonline.net

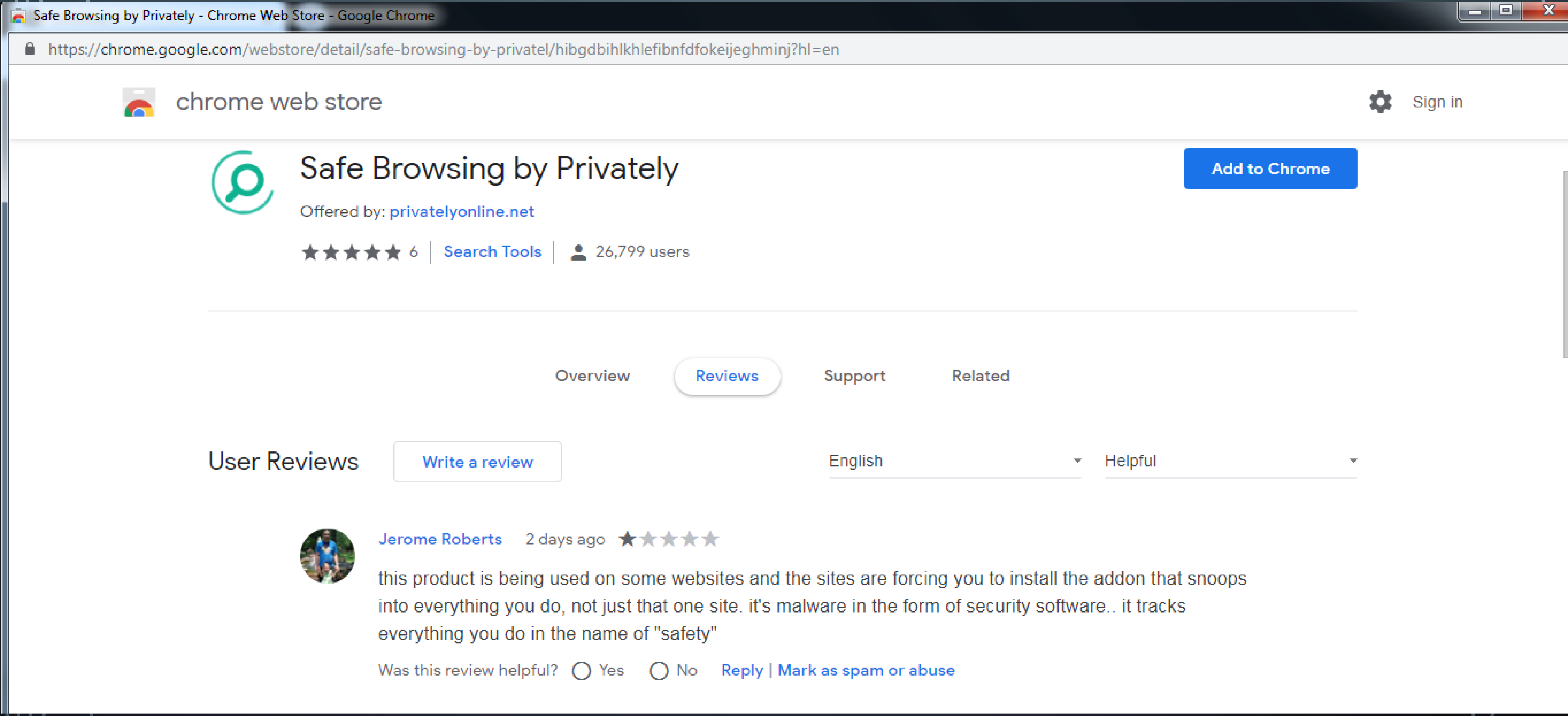
★★★★★ 6 | Search Tools | 26,799 users

You completed the security check

Almost there... Click **Add** to continue

By clicking the button above and installing Safe Browsing by Privately Chrome extension, I accept and agree to abide by the **Terms and Conditions** and **Privacy Policy**

Copyright © 2018 Privately | Privacy Policy | Terms and Conditions


Safe Browsing by Privately - Chrome Web Store - Google Chrome
https://chrome.google.com/webstore/detail/safe-browsing-by-privatel/hibgdbihlkhlefibnfdfokeijeghminj?hl=en
chrome web store
Sign in
Add to Chrome
Overview
Reviews
Support
Related
Write a review
English
Helpful

Safe Browsing by Privately

Offered by: privatelyonline.net

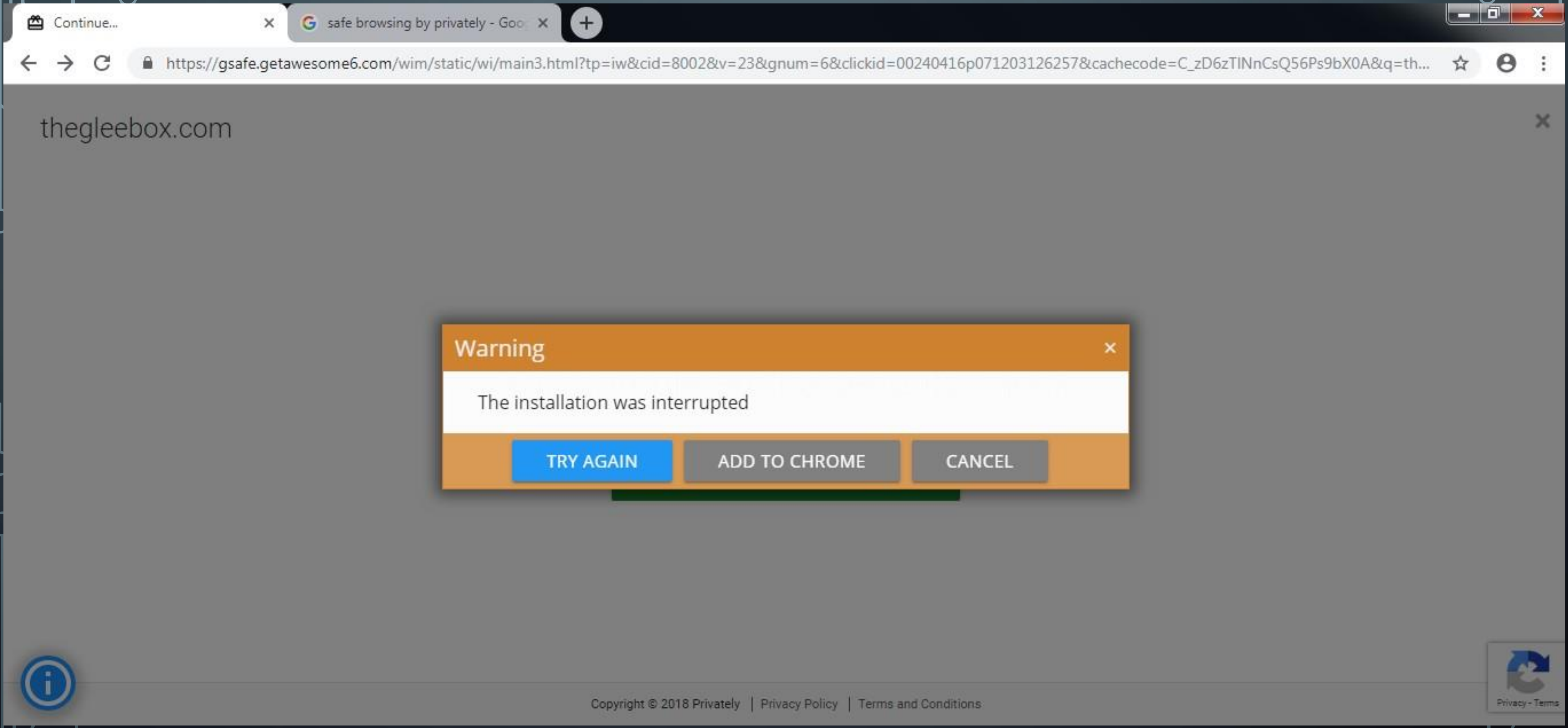
★★★★★ 6 | Search Tools | 26,799 users

User Reviews

Jerome Roberts 2 days ago ★☆☆☆☆

this product is being used on some websites and the sites are forcing you to install the addon that snoops into everything you do, not just that one site. it's malware in the form of security software.. it tracks everything you do in the name of "safety"

Was this review helpful? ○ Yes ○ No Reply | Mark as spam or abuse



Continue...
safe browsing by privately - Goo
https://gsafe.getawesome6.com/wim/static/wi/main3.html?tp=iw&cid=8002&v=23&gnum=6&clickid=00240416p071203126257&cachecode=C_zD6zTINnCsQ56Ps9bX0A&q=th...
thegleebox.com

Warning

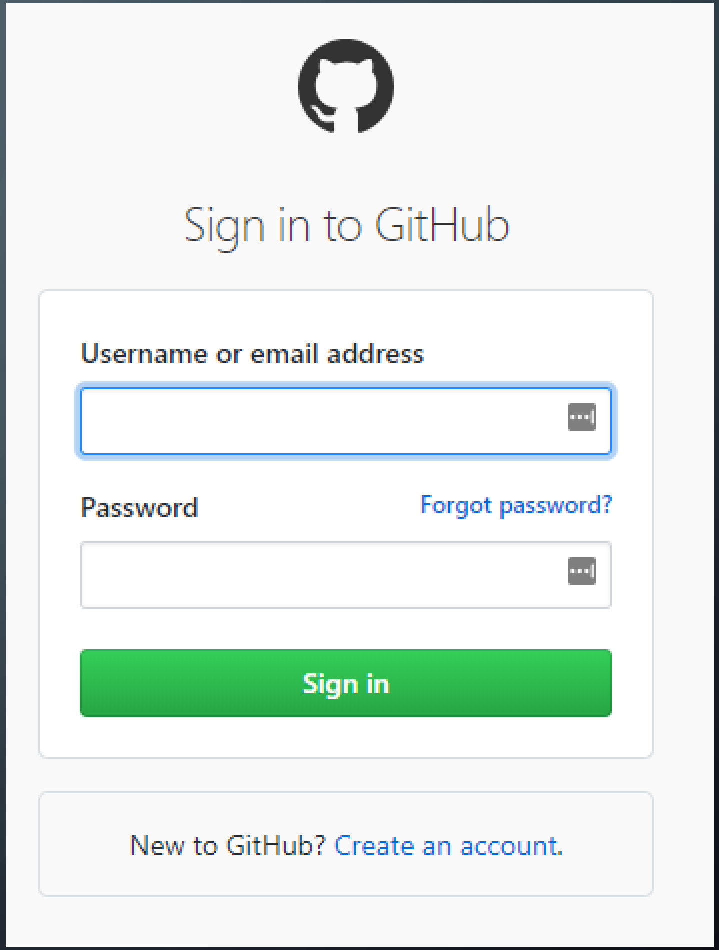
The installation was interrupted

TRY AGAIN
ADD TO CHROME
CANCEL

Copyright © 2018 Privately | Privacy Policy | Terms and Conditions

OR YOU COULD END UP HERE

- Github sign-in phishing page
  - Using Social Engineering Toolkit Credential Harvester
- Or any other organization’s sign-in page



Sign in to GitHub

Username or email address

Password

New to GitHub? Create an account.

ATTACK SCENARIO

- Don’t try this at home! This is for research and educational purposes only…
- One positive/negative of red team thinking is always trying to find a way to turn something into an attack
  - White hat hackers then teach others how to watch out and avoid the attack methods

ATTACK SCENARIO

- What if a email was spoofed to look like it came from a coworker?
  - For an issue that you were currently having trouble with
  - Or about a topic that interested you
- What if the email contained a link to a legitimate organization’s blog post?
- What if a link in the blog post went to a once legitimate website that lapsed registration?
- What if an attacker took over ownership of the linked website?

ATTACK STEPS

- Find an expired domain that is linked to in an organization's old blog post
    - Scrape through old blog posts
    - Visit any links in the blog posts
- Register the domain, create a phishing page at the domain
- Make a phishing email based on the blog post contents, to convince the user to click on the link in the blog post

ATTACK STEPS

- On the phishing domain
  - Infect the user with malware
  - Or present the user with the organization’s sign-in page, to harvest their credentials

TAKE AWAYS

- This is not just a Github blog issue. It can happen to any organization's old/forgotten webpage
- Be cautious when click on links, even on legitimate websites
  - Dead sites can get bought by an attacker
  - An attacker can change DNS to redirect a domain to an attack website
  - Malware can be injected into the site
    - Through outdated website software
    - Through 3rd party scripts (target one central source, attack many endpoints)

NOTE FOR BUG BOUNTIES

- When submitting a report for a bug bounty, always list the highest severity vulnerability first
    - I first submitted the bug findings report with 200 dead links listed first, and then 2 active phishing links. But the bug bounty closed the report as a known issue.
    - I then submitted the bug findings report with the 2 active phishing links listed first, and then the dead links. The bug bounty paid out for this report.

NOTE FOR BUG BOUNTIES, CONT.

- Don’t be surprised if the organization does not fix or clean up the issue right away.
  - Security is just part of an organization’s needs.
  - If the security threat does not outweigh the risk, they might choose to not fix the issue.
- Github said that they were aware of the issue about stale links, but they were not going to fix it at that point because they didn’t have time.
  - However, the phishing and stale links that I reported were removed sometime between November 2018 and March 2019.

TIPS FOR RESEARCH / BUG FINDING

- Try to change or corrupt input, and see what the website or app does
- Try to use a website or app incorrectly, and see what it does
- Look for accidental information disclosure
  - Pictures on a wall, image on a monitor, etc